http://vestnik.mrsu.ru
ISSN Print 2658-4123
ISSN Online 2658-6525

УДК 004.415.538 DOI: 10.15507/2658-4123.029.201901.020-039

# Системно-динамическое моделирование сетевых информационных операций

**В. А. Минаев[1*], М. П. Сычев[1], Е. В. Вайц[1], К. М. Бондарь[2]**

*[1]ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана» (г. Москва, Россия)*
*[2]ФГКОУ ВО «Дальневосточный юридический институт МВД РФ» (г. Хабаровск, Россия)*
*[*]m1va@yandex.ru*

*Введение.* В Доктрине информационной безопасности Российской Федерации основными негативными факторами, влияющими на состояние информационной безопасности, названы информационно-технические и информационно-психологические воздействия. Поэтому моделирование, оценка и прогнозирование информационных воздействий на социальные группы и организация соответствующего информационного противодействия являются актуальными задачами управления.
*Материалы и методы.* Рассмотрены системно-динамические модели информационных воздействий в социальных сетях и группах. Обосновано их применение с целью противодействия информационному терроризму и экстремизму. Дано описание в виде потоковых диаграмм в обозначениях системной динамики. Приведены системы дифференциальных уравнений. Проведены эксперименты с моделями с применением перспективной имитационной платформы Anylogic.
*Результаты исследования.* Произведено сравнение агентной и системно-динамической модели, показавшее высокую степень их согласования между собой и со статистическими данными. С использованием реальных данных на основе метода кластерного анализа выделены типологические группы в выборочной совокупности поселений России с различающимся средним временем распространения информационных воздействий. Успешно апробированы системно-динамические модели распространения информационных воздействий в социальных сетях и в студенческой среде с использованием постулата Гиббса.
*Обсуждение и заключение.* Показана высокая согласованность результатов моделирования с эмпирическими данными (коэффициенты детерминации не менее 90 %). Модели позволяют осуществлять прогноз информационного воздействия и информационного противодействия, проигрывать различные сценарии динамики указанных процессов.

***Ключевые слова:*** имитационное моделирование, терроризм, экстремизм, информационное воздействие, информационное противодействие, управление, социальная сеть, топология, типология, кластерный анализ

***Для цитирования:*** Системно-динамическое моделирование сетевых информационных операций / В. А. Минаев [и др.] // Инженерные технологии и системы. 2019. Т. 29, № 1. С. 20–39. DOI: https://doi.org/10.15507/2658-4123.029.201901.020-039

# System-Dynamic Modeling of Network Information Operations

**V. A. Minaev[1*], M. P. Sychev[1], E. V. Vaits[1], K. M. Bondar[2]**
*[1]Bauman Moscow State Technical University (Moscow, Russia)*
*[2]Far Eastern Law Institute of the Ministry of Internal Affairs of the Russia (Khabarovsk, Russia)*
*[*]m1va@yandex.ru*

*Introduction.* Information-technical and information-psychological influences are the main negative factors affecting the information security according to the Information Security Doctrine of the Russian Federation. Therefore, modeling, evaluating and forecasting information influences on social groups and organizing adequate information counteraction are urgent tasks of management.
*Materials and Methods.* The system-dynamic models of information influences in social networks and groups are considered. Their application for purposes of counteraction to information terrorism and extremism is proved. The description in the form of flowcharts is given. Systems of differential equations are presented. Experiments with models using the advanced simulation platform Anylogic have been carried out.
*Results.* In a sample of Russian settlements based on the cluster analysis there have been found homogeneous typological groups that differ in the average time of disseminating information in social networks. Based on Gibbs's Postulate, the system-dynamic model of information influences on students has been successfully tested.
*Discussion and Conclusion.* The high consistency of simulation results with empirical data (determination coefficients of at least 90 %) is shown. Models allow forecasting the information influence and information counteraction and playing different scenarios for the dynamics of these processes.

***Keywords:*** simulation modeling, terrorism, extremism, information influence, information counteraction, management, social network, topology, typology, cluster analysis

***For citation:*** Minaev V.A., Sychev M.P., Vaits E.V., Bondar K.M. System-Dynamics Modeling of Network Information Operations. *Inzhenernyye tekhnologii i sistemy* = Engineering Technologies and Systems. 2019; 29(1):20-39. DOI: https://doi.org/10.15507/2658-4123.029.201901.020-039

## Введение

Основными негативными факторами, влияющими на состояние информационной безопасности России, в новой Доктрине информационной безопасности Российской Федерации названы информационно-технические (ИТВ) и информационно-психологические воздействия (ИПВ)[1]. Так, в Доктрине отмечается наращивание рядом зарубежных стран возможностей информационно-технического воздействия (ИТВ) на информационную инфраструктуру в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса. В частности, возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере; увеличивается количество все более изощренных преступлений, связанных с неприкосновенностью частной жизни, личной и семейной тайны при обработке персональных данных.

Одновременно в Доктрине указывается на расширение масштабов использования зарубежными спецслужбами информационного воздействия, направленного на дестабилизацию внутриполитической и социально-экономиче-

[1] Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ № 646 от 5 декабря 2016 г. № 646. URL: http://base.garant.ru/71556224

ской ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. Россия не является исключением.

В Доктрине отмечено, что:

– в целях размывания традиционных российских духовно-нравственных ценностей наращивается информационное воздействие на население России, в первую очередь на молодежь;

– террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание для нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии.

**Обзор литературы**

К настоящему времени актуализировались интенсивные исследования в области анализа, моделирования и прогнозирования негативных информационных воздействий (ИВ) и информационных противодействий (ИПД) им [1–4].

Появились новые научные работы, отражающие распространение таких воздействий с помощью компьютерных сетей в различных социальных средах (школьных, студенческих, фанатских и др.); различных поселениях: мегаполисах с их специфическими малыми группами, несущими опасность для молодых людей (группы самоубийц, этнические криминальные группы, руферы, диггеры, зацеперы в метро и др.); малых и моногородах (с тотальной безработицей и аморальными образцами поведения среди взрослых) [5].

Вышеизложенное позволяет заключить, что моделирование, оценка и прогнозирование информационных воздействий на социальные группы и организация соответствующего информационного противодействия являются актуальными задачами управления.

К настоящему моменту создана обширная научная база в сфере моделирования информационных воздействий на социальные группы во времени, позволяющая исследовать информационное «заражение» в зависимости от влияния различных внешних и внутренних факторов [1–5].

Разработаны и исследованы различные типы моделей в сфере информационного воздействия: топологические, факторные, регрессионные, вероятностные и др., которые составляют основу для дальнейшего совершенствования инструментария моделирования в сфере информационного воздействия на социум.

В то же время наиболее интересные с практической точки зрения имитационные методы моделирования информационных воздействий на социальные группы и соответствующего информационного противодействия, позволяющие проигрывать различные сценарии проведения информационных операций, в России недостаточно развиты; слабо ведется разработка необходимого комплекса моделей.

**Материалы и методы**

Исходя из вышеизложенного, можно выделить два важных направления разработки моделей информационных операций, связанных с ИТВ с одной стороны и с ИПВ – с другой. Кроме того, процесс моделирования был бы неполон, если бы не рассматривались модели противодействия ИТВ и ИПВ. В табл. 1 показана степень разработанности названных моделей информационных операций, оцененная в ходе экспертного опроса по 10-балльной шкале (в нем участвовали 45 квалифицированных экспертов).

В данной статье рассмотрены базовые модели в последних двух направлениях (менее разработанных) и некоторые результаты их применения.

Созданы и реализованы математические модели, позволяющие имити-

Таблица 1
Table 1

**Степень разработанности моделей информационных операций**
**Readiness level of information operation models**

| Модели информационных операций / Models of information operations | Модели ИТВ / Models of informational and technical impacts (ITI) | Модели противодействия ИТВ / Models of ITI counteraction | Модели ИПВ / Models of informational and psychological impacts (IPI) | Модели противодействия ИПВ / Models of IPI counteraction |
|---|---|---|---|---|
| Степень разработанности моделей (баллы) / Level of models readiness (in points) | 7 | 5 | 5 | 3 |

ровать ИПВ и ИПД в социальных сетях и при непосредственном общении индивидов в разнообразных общественных группах. При этом применяется перспективная программная платформа имитационного моделирования Anylogic, на основе которой реализованы модели с высокими коэффициентами объясняемости (не менее 85–90 %) между эмпирическими и модельными данными [6].

Созданная методологическая и методическая база позволяет расширить поле исследований информационных воздействий и создания моделей информационных взаимодействий при проявлениях экстремизма, терроризма и агрессивного поведения социальных групп, включая обучающихся в образовательных организациях. Для этого необходимо решить три основные задачи:

– обосновать и построить базу данных, позволяющую по сетевому информационному контенту распознавать и визуализировать ситуации возникновения агрессивного поведения тех или иных групп населения. К настоящему времени разработаны современные методы анализа контента, позволяющие выявлять инициаторов такого контента и сетевые узлы, которые с инициаторами связаны;

– изучить и спрогнозировать динамику «заражения» обучающихся стереотипами агрессивного поведения. Для этого целесообразно комплексно использовать методы системно-динамического, агентного и дискретно-событийного моделирования[2];

– создать распределенную информационно-аналитическую систему (ИАС) мониторинга агрессивного поведения в регионах Российской Федерации с выделением в указанной системе региональных ситуационных центров, где происходила бы оперативная обработка информации и принятие специалистами решений по возникающим случаям «экстремального напряжения» в социальной среде, включая ее молодежную часть.

По сути, речь идет о построении глобальной информационной системы мониторинга в масштабах страны, которая дает возможность:

– обеспечения своего развития путем включения в нее (по мере готовности и необходимости) модулей мониторинга проявлений экстремизма, терроризма и других социально опас-

[2] **Маликов Р. Ф.** Практикум по имитационному моделированию сложных систем в среде AnyLogic 6 : учеб. пособ. Уфа : Изд-во БГПУ, 2013. 296 с.

ных явлений, а также модулей подготовки управленческих решений для региональных органов власти и силовых структур при реагировании на подобные явления и ситуации;

– использования перспективных программно-математических средств и методов при реализации механизмов комплексного реагирования на проявления агрессивного поведения;

– надежной защиты центров информационного доступа и коммуникационных каналов ИАС.

Учитывая масштабность и острую социальную необходимость реализации на современном уровне механизмов комплексного реагирования на проявления агрессивного поведения (данная проблема, судя по мировым трендам, может только усиливаться), создание высокоорганизованной ИАС связано с привлечением для ее развития высокопрофессиональных специалистов из разных сфер деятельности (математиков, психологов, педагогов, психиатров, представителей информационной сферы, специалистов в области защиты информации и др.).

Приведем необходимые определения, относящиеся к предмету, цели и задачам данной статьи.

Уточняя терминологию работы С. П. Расторгуева и М. В. Литвиненко[3], определим *сетевые информационные операции* как комплекс взаимосвязанных целенаправленных действий информационного характера, осуществляемых в компьютерных сетях и массмедиа посредством межличностных контактов и ориентированных на решение задач по перепрограммированию, блокированию, генерации информационных процессов как в технической, так и в гуманитарной сферах.

*Системно-динамическое моделирование* – метод моделирования и имитации сложных динамических систем, характеризующихся разветвленными, как правило, нелинейными связями [7]. Системная динамика как новое направление в области моделирования получила свое развитие благодаря:

– успехам в области анализа и проектирования сложных систем управления;

– прогрессу в сфере компьютерного моделирования и вычислительных методов.

Базовые работы в этом направлении относятся к исследованиям Дж. Форрестера конца 50-х – начала 60-х гг. XX в., посвященных анализу промышленных предприятий[4], развитию городов[5] и мировой динамике[6].

К настоящему времени построением системно-динамических моделей в области информационной безопасности занимаются различные зарубежные научные коллективы: в Университете Карнеги (Меллон, США)[7], Оборонном научно-техническом университете Народно-освободительной армии Китая [8], Высшей школе информационной безопасности (Южная Корея) [9], Флоридском Атлантическом университете (США) [10] и в других научных центрах мира.

Созданные за рубежом модели успешно применяются на практике, однако требуют концептуальной и методи-

[3] **Расторгуев С. П., Литвиненко М. В.** Информационные операции в сети Интернет / Под общ. ред. А. Б. Михайловского. М. : АНО ЦСОиП, 2014. 128 с.

[4] **Форрестер Дж.** Основы кибернетики предприятия (индустриальная динамика) / Пер. с англ. ; общ. ред. и предисл. Д. Гвишиани. М. : Прогресс, 1971. 340 с.

[5] **Форрестер Дж.** Динамика развития города / Пер. с англ. М. Орловой ; под ред. Ю. Иванилова, А. Иванова, Р. Оганова ; предисл. Ю. Козлова. М. : Прогресс, 1974. 286 с.

[6] **Форрестер Дж.** Мировая динамика / Пер. с англ. А. Ворощука, С. Пегова ; послесл., коммент. Н. Моисеева. М. : Наука, 1978. 384 с.

[7] Management and education of the risk of insider threat (MERIT): system dynamics modeling of computer system sabotage / D. M. Cappelli [et al.]. Pittsburg : Carnegie Mellon University. Software Engineering Institute, 2006. 34 p. URL: https://www.semanticscholar.org/paper/Management-and-Education-of-the-Risk-of-Insider-(-)-Cappelli/7fbad6a22afe183e63fb1bb8834e7de05a5d4d94

ческой доработки и дополнительных исследований для решения задач анализа, оценки, прогнозирования и управления в сфере информационных воздействий и информационного противоборства.

В основе моделей системной динамики лежат общие структурные элементы, пригодные для моделирования многих систем[8–10]:

– *уровни* – управляемые объекты, отображаемые переменными, значения которых представляют интегральные характеристики некоторых реальных потоков, рассматриваемых в моделируемой системе;

– *темпы* – скорости потоков, исходящих от одних уровней и входящих в другие, вызывая в них соответствующие изменения.

Кроме того, в моделях используются *функции решений*, определяемые через функциональные зависимости, существующие в системе; *вспомогательные величины и константы*.

Системная динамика, представляя собой определенную целостность принципов и методов анализа динамических управляемых систем с обратной связью, дает возможность их применения для решения многих организационно-производственных и социально-экономических задач.

Метод системной динамики предполагает, что для основных фазовых переменных (*системных уровней*) используются дифференциальные уравнения типа [11]:

$$\dot{y} = y^{+} - y^{-}, \qquad (1)$$

где $\dot{y}$ – производная переменной $y$ по времени; $y^{+}$ – комплекс факторов, положительно сказывающихся на скорости изменения уровня $y$; $y^{-}$ – комплекс факторов, отрицательно сказывающихся на скорости изменения уровня $y$.

В моделях Форрестера предполагается, что $y^{\pm}$, в свою очередь, являются функциями уровней

$$y^{\pm} = f(F_1, F_2, ..., F_k), \qquad (2)$$

где $k$ – количество факторов меньшее, чем количество фазовых переменных; каждый фактор зависит только от части системных уровней.

*Системно-динамическая модель ИВ*

На рис. 1 приведено описание системно-динамической модели ИВ с обозначениями, рассматриваемыми в системе дифференциальных уравнений (3).

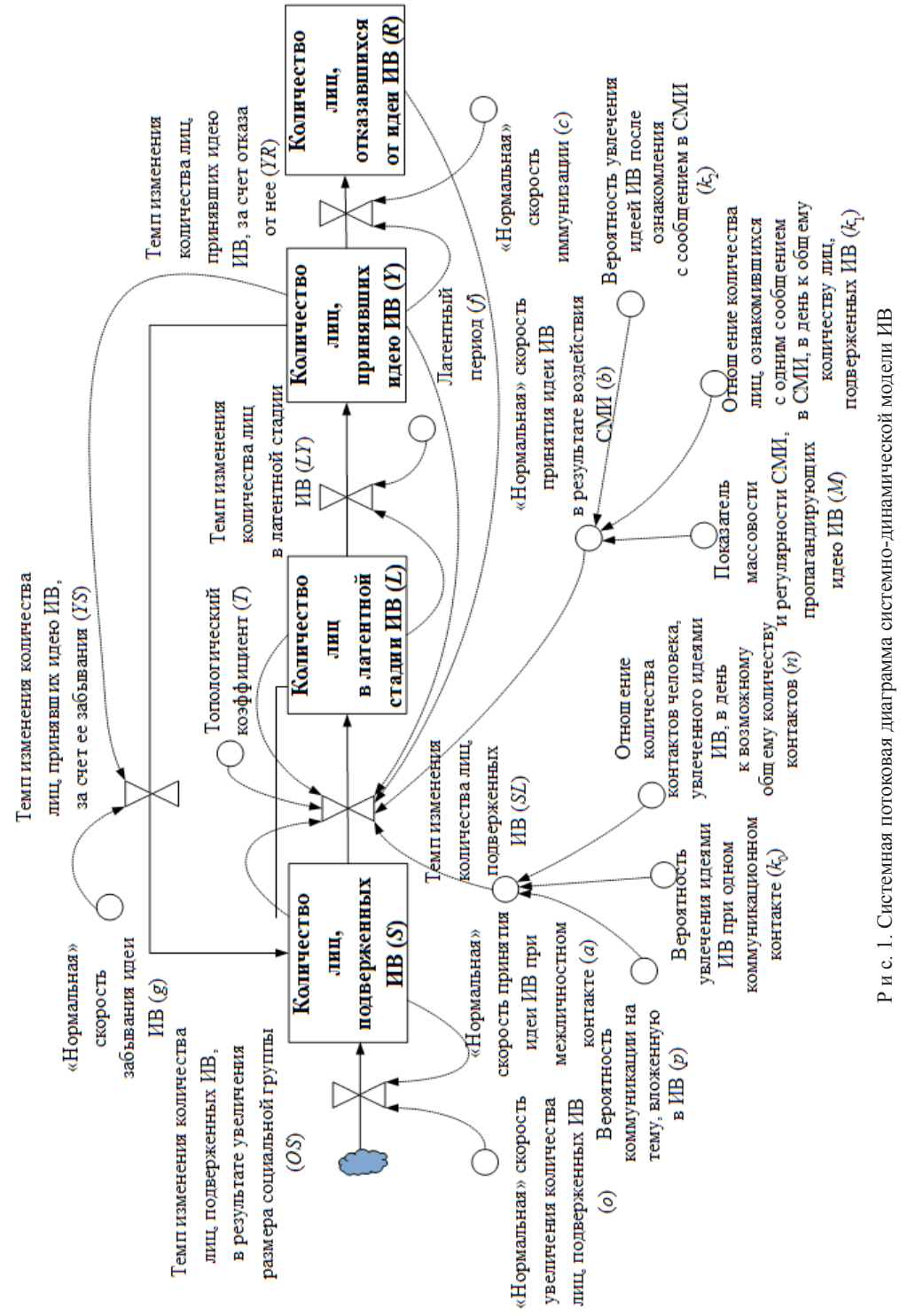
$$\begin{cases} \dfrac{dS}{dt} = OS(t) + YS(t) - SL(t) \\ \dfrac{dY}{dt} = SL(t) - LY(t) \\ \dfrac{dR}{dt} = LY(t) - YR(t) - YS(t) \\ OS(t) = o \cdot S(t) \\ SL(t) = b \cdot S(t) + \dfrac{a \cdot T \cdot S(t) \cdot Y(t)}{S(t) + Y(t) + L(t) + R(t)} \\ YR(t) = c \cdot Y(t) \\ LY(t) = \dfrac{L(t)}{f} \\ YS(t) = g \cdot Y(t) \\ a = p \cdot k_0 \cdot n \\ b = M \cdot k_1 \cdot k_2 \end{cases} \qquad (3)$$

Построение системно-динамической модели ИПД связано с моделью ИВ на социальные группы. Предпола-

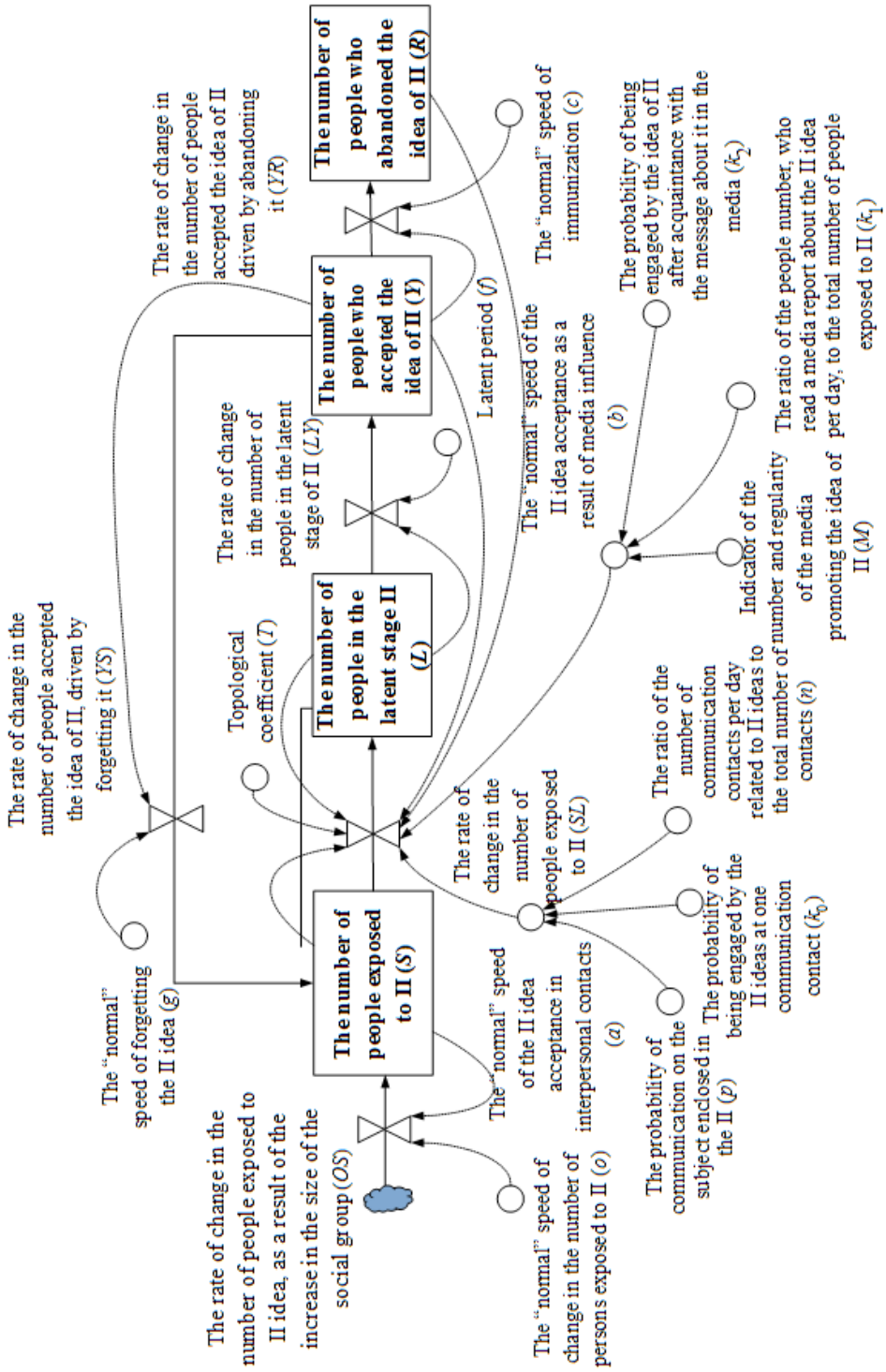
[8] **Форрестер Дж.** Основы кибернетики предприятия (индустриальная динамика) / Пер. с англ. ; общ. ред. и предисл. Д. Гвишиани. М. : Прогресс, 1971. 340 с.

[9] **Форрестер Дж.** Динамика развития города / Пер. с англ. М. Орловой ; под ред. Ю. Иванилова, А. Иванова, Р. Оганова ; предисл. Ю. Козлова. М. : Прогресс, 1974. 286 с.

[10] **Форрестер Дж.** Мировая динамика / Пер. с англ. А. Ворощука, С. Пегова ; послесл., коммент. Н. Моисеева. М. : Наука, 1978. 384 с.




Р и с. 1. Системная потоковая диаграмма системно-динамической модели ИВ




F i g. 1. The system flow diagram of the information influence system-dynamic model

гается, что в социуме одновременно идет распространение двух противоположных идей ИВ (положительной и отрицательной). Потоковая диаграмма, описывающая системно-динамическую модель ИПД, будучи представленной системой дифференциальных уравнений (4), приведена на рис. 2.

$$\begin{cases} \frac{dS}{dt} = OS(t) + XS(t) + YS(t) - SX(t) - SY(t) \\ \frac{dX}{dt} = SX(t) + YX(t) - XS(t) - XY(t) \\ \frac{dY}{dt} = SY(t) + XY(t) - YS(t) - YX(t) \\ SX(t) = b_x \cdot S(t) + \frac{a_x \cdot S(t) \cdot X(t)}{S(t) + X(t) + Y(t)} \\ SY(t) = b_y \cdot S(t) + \frac{a_y \cdot S(t) \cdot Y(t)}{S(t) + X(t) + Y(t)} \\ XY(t) = \frac{k_x \cdot X(t) \cdot Y(t)}{X(t) + Y(t)} \\ YX(t) = \frac{k_y \cdot X(t) \cdot Y(t)}{X(t) + Y(t)} \\ XS(t) = g_x \cdot X(t) \\ YS(t) = g_y \cdot Y(t) \\ OS(t) = o \cdot S(t). \end{cases} \quad (4)$$

Для практической реализации системно-динамических моделей ИВ и ИПД использовались статистические данные о распространении различных информационных воздействий в социальных сетях, а также данные опросов в социальных группах. Отметим, что процесс имитационного моделирования, осуществленный с использованием современной программной платформы Anylogic, позволяет «проигрывать» любое количество противоборствующих идей[11]. Основными переменными, динамика которых в социуме отслеживалась с помощью разработанных моделей, является количество лиц:

– подверженных ИВ;

– находящихся в латентной стадии ИВ;

– принявших идею ИВ;

– отказавшихся от идеи ИВ.

При этом системно-динамическая модель ИПД, являющаяся логическим развитием модели ИВ, учитывает характеристики забывания информации, существования латентного периода, изменения размера социальной группы, топологию взаимодействия в группе, замещения идеи ИВ идеей противоборствующей стороны.

**Результаты исследования**

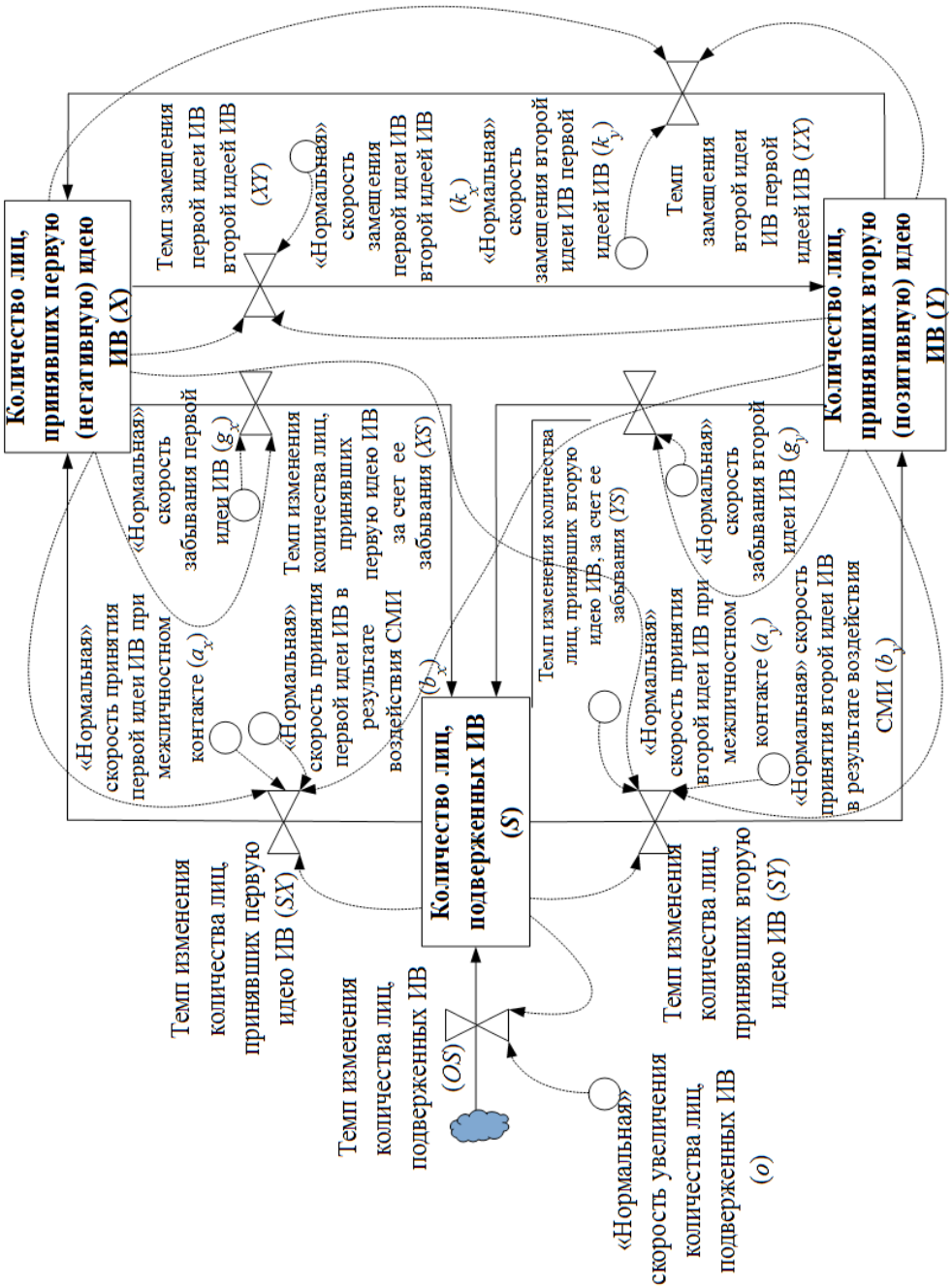
Результаты некоторых модельных экспериментов по изучению влияния различных параметров на динамику процессов ИВ приведены на рис. 3–5. Пример имитационного эксперимента с системно-динамической моделью ИПД приведен на рис. 6.

Отметим, что результаты моделирования на основе системно-динамического и агентного подходов совпали с достаточной степенью точности (рис. 7). Коэффициент согласования между моделями составил 94 %, со статистическими данными – 92 %.

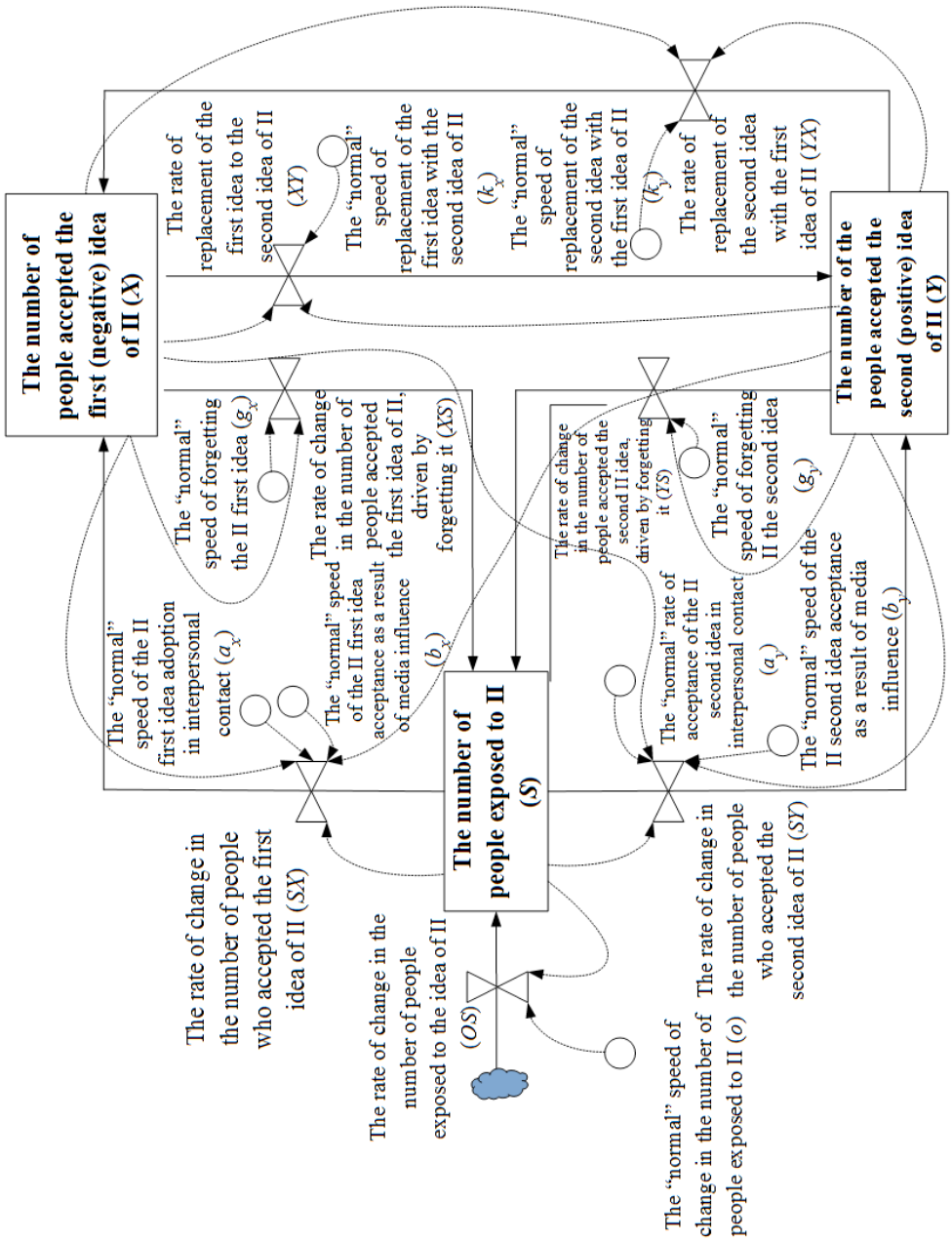
В экспериментах на материале фактических статистических данных имитировалось по отдельности распространение ИВ от семи различных пользователей, а также одновременно с нескольких узлов реальной социальной сети (рис. 8).

Из рис. 8 следует, что динамика количества лиц, «зараженных» идей ИВ, в зависимости от источника «заражения» в г. К. различается, подчиняясь общим динамическим закономерностям логистического характера.

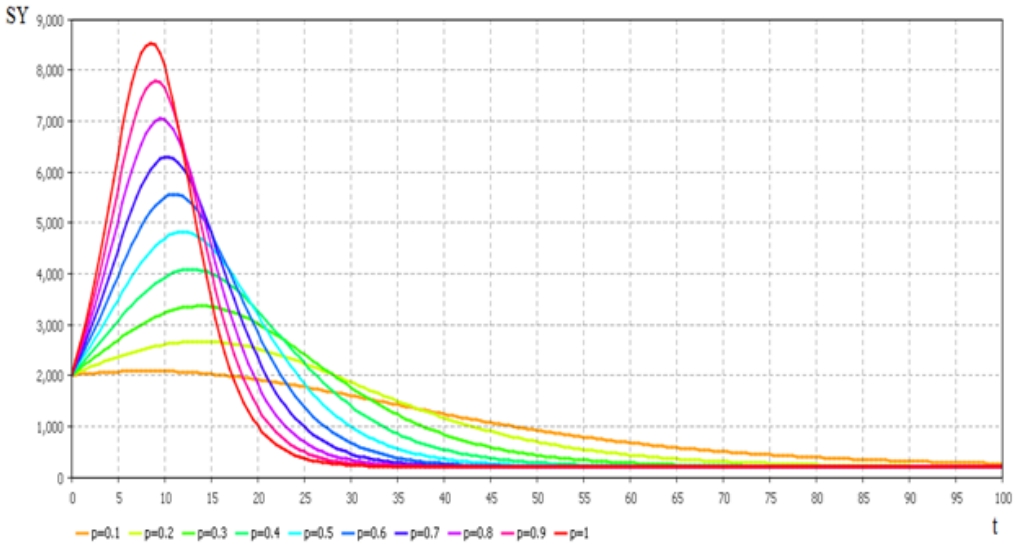
[11] **Лычкина Н. Н.** Современные технологии имитационного моделирования и их применение в информационных бизнес-системах и системах поддержки принятия решений // Имитационное моделирование. Теория и практика : сб. докл. 2-й Всерос. науч.-практ. конф. ИММОД-2005. Т. 1. СПб. : ЦНИИТС, 2005. С. 25–31. URL: https://www.anylogic.ru/upload/iblock/efa/efac2601a53aa4a5c810fb1c2f8fa79b.pdf




Р и с. 2. Системная потоковая диаграмма системно-динамической модели ИПД

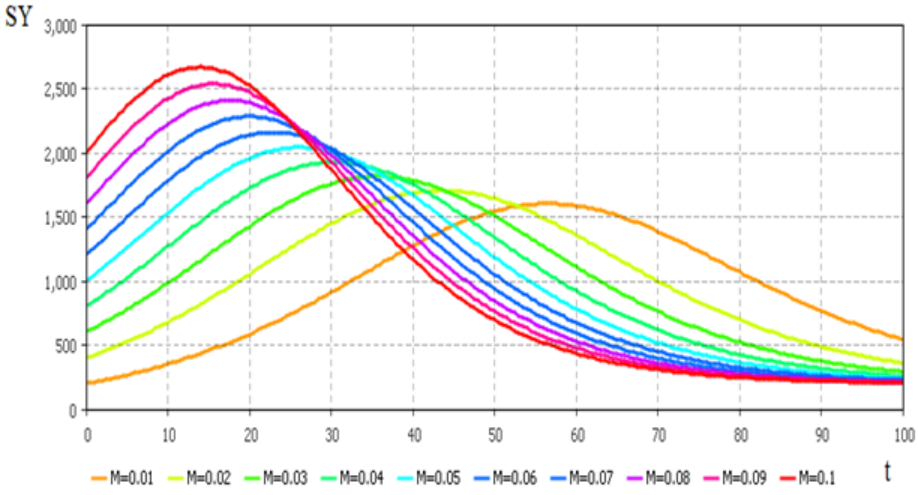



F i g. 2. The system flow diagram of the system-dynamic model of information and psychological counteractions



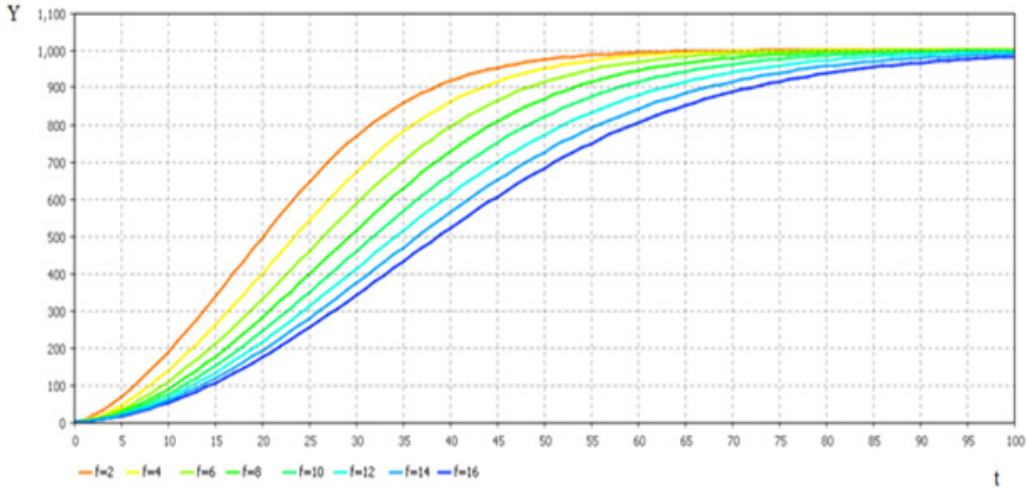

Р и с. 3. Скорость принятия идеи ИВ (*SY*) в зависимости от вероятности коммуникации на тему, вложенную в контент ИВ (*p*)

F I g. 3. The speed of acceptance of the II idea (*SY*) depending on the probability of communication on the topic, related to II content (*p*)



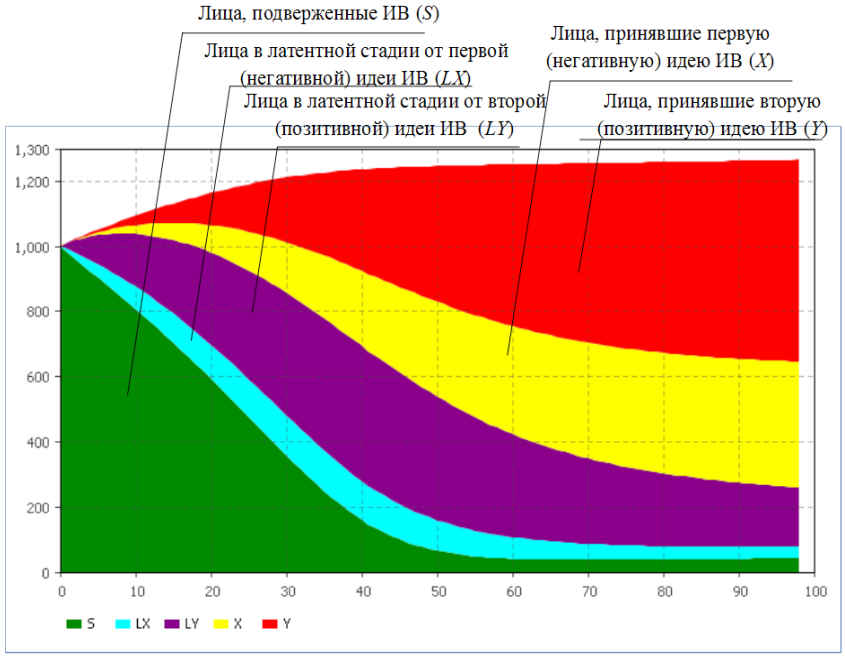

Р и с. 4. Скорость принятия идеи ИВ (*SY*) в зависимости от показателя массовости и регулярности СМИ, пропагандирующих идею ИВ (*M*)

F i g. 4. The speed of acceptance (*SY*) of the II idea depending on the circulation and regularity (*M*) of the media promoting it

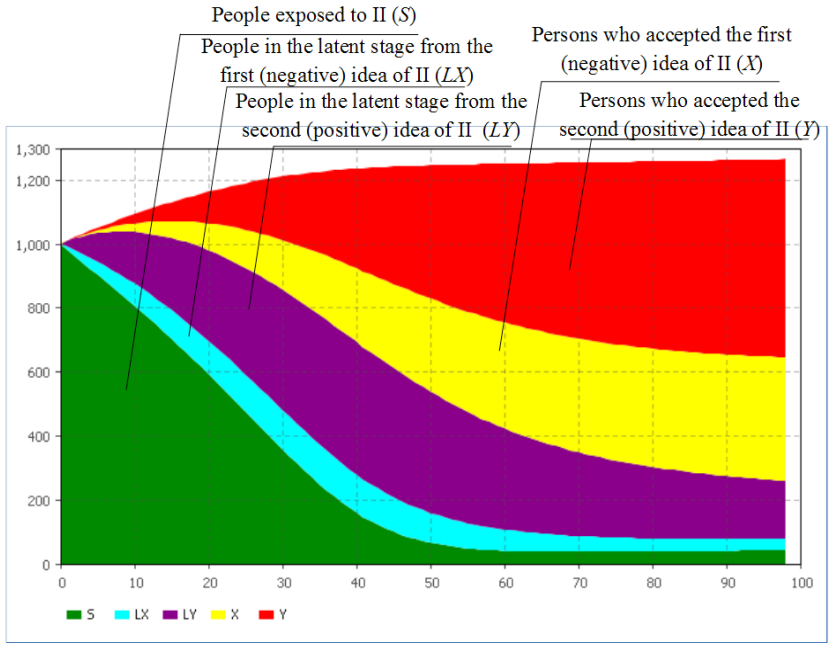



Р и с. 5. Динамика количества лиц, принявших идею ИВ (*Y*), в зависимости от длительности латентного периода (*f*)

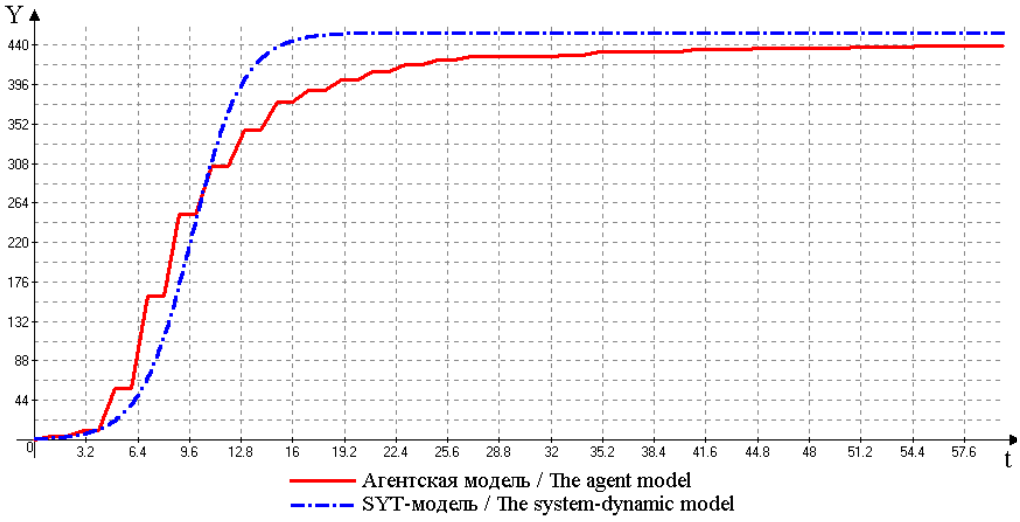
F i g. 5. The dynamics of the number of people who accepted the II idea (*Y*), depending on the duration of the latent period (*f*)




Р и с. 6. Динамика количества лиц, подверженных ИВ (*S*), принявших первую – негативную (*X*) и вторую – позитивную (*Y*) идеи ИВ, а также лиц в латентной стадии от первой (*LX*) и второй (*LY*) идей ИВ

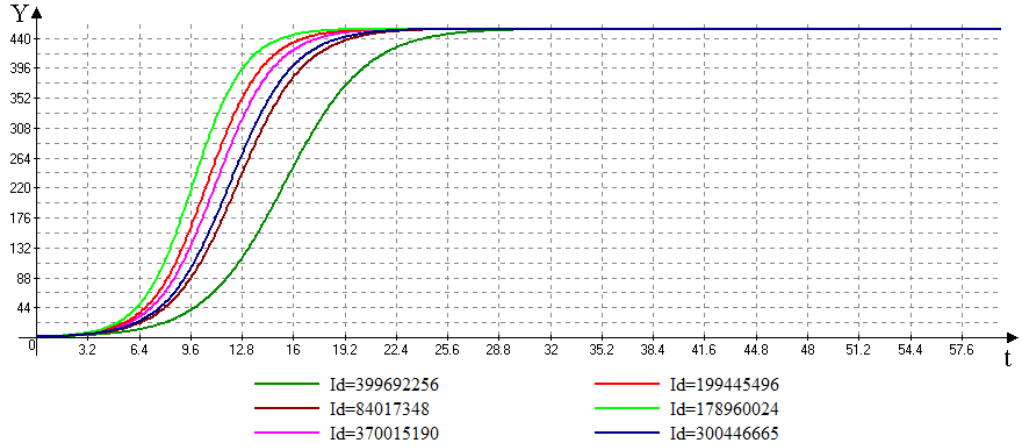



F i g. 6. The dynamics of the number of people exposed to II (*S*), the first – negative (*X*) and second – positive (*Y*) ideas, as well as people in the latent stage of the first (*LX*) and second (*LY*) ideas




Р и с. 7. Результаты сравнительного моделирования ИВ на основе системно-динамического и агентного подходов

F i g. 7. The results of comparative modeling of II based on the system-dynamic and agent approaches




Р и с. 8. Динамика количества лиц, «зараженных» идеей ИВ, в зависимости от источника «заражения» в г. К.

F i g. 8. The dynamics of the number of people, “infected” with the II idea, depending on the infection source in the city of K

Далее эксперимент был расширен: в качестве объектов исследования были выбраны 42 малых города России. По результатам анализа данных о сетевых связях между пользователями социальной сети «ВКонтакте» построены отображающие их графы. Рассчитаны топологические характеристики социальных сетей, такие как коэффициент кластеризации, степень связности, диаметр, плотность, средняя длина пути.

С целью выделения однородных групп поселений для сравнения времени распространения ИВ в них, исходя из топологических характеристик, применен иерархический метод кластерного анализа – метод Вальда. Дендрограмма кластеризации представлена на рис. 9.

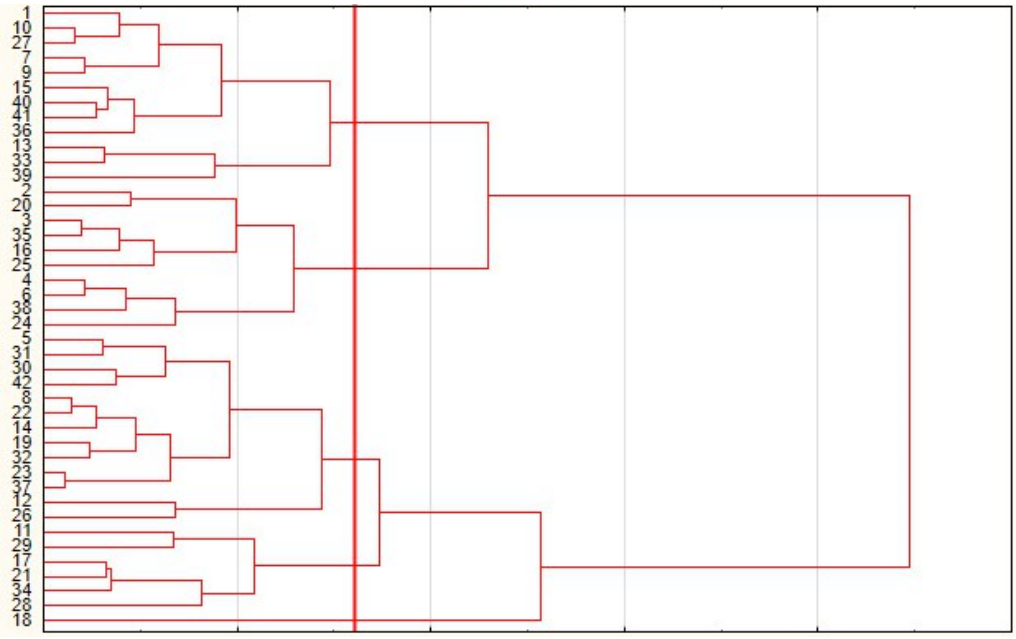
В табл. 2 показано среднее время распространения ИВ в различных кластерах. Ее анализ свидетельствует о том, что наблюдается существенное различие среднего времени распространения ИВ в кластерах.

Данное обстоятельство требует различной стратегии и тактики со стороны соответствующих государственных структур по организации информационного противоборства в поселениях, относящихся к различным типологическим группам. Это в полной мере относится к сфере борьбы с терроризмом и экстремизмом в информационной среде.

Для апробации моделей далее был проведен эксперимент по результатам анализа статистических данных по сообществу в социальной сети «ВКонтакте», которое было создано с целью организации реального политического митинга с экстремистскими лозунгами. Временные зависимости, полученные по результатам моделирования, показывают высокую объясняемость модели; коэффициент детерминации равен 95 % (рис. 10). Отметим, что в динамике распространения ИВ о проведении оппозиционных митингов выделяются два периода с разными параметрами модели ИВ, соответствующими двум информационным вбросам, произошедшим в российских городах в тот период.

В рамках исследований по моделированию ИВ также проведен важный эксперимент, подтвердивший известный постулат Гиббса о статистических ансамблях[12]. Существо постулата в том,

[12] **Гиббс Дж.** Основные принципы статистической механики, излагаемые со специальным применением к рациональному обоснованию термодинамики / Пер. с англ. К. В. Никольского. М. ; Л. : Гостехиздат, 1946. 203 с.




Р и с. 9. Типологические группы выборочной совокупности поселений России

F i g. 9. Typological groups of a sample of Russian settlements

Т а б л и ц а 2

T a b l e 2

**Среднее время распространения ИВ в кластерах**

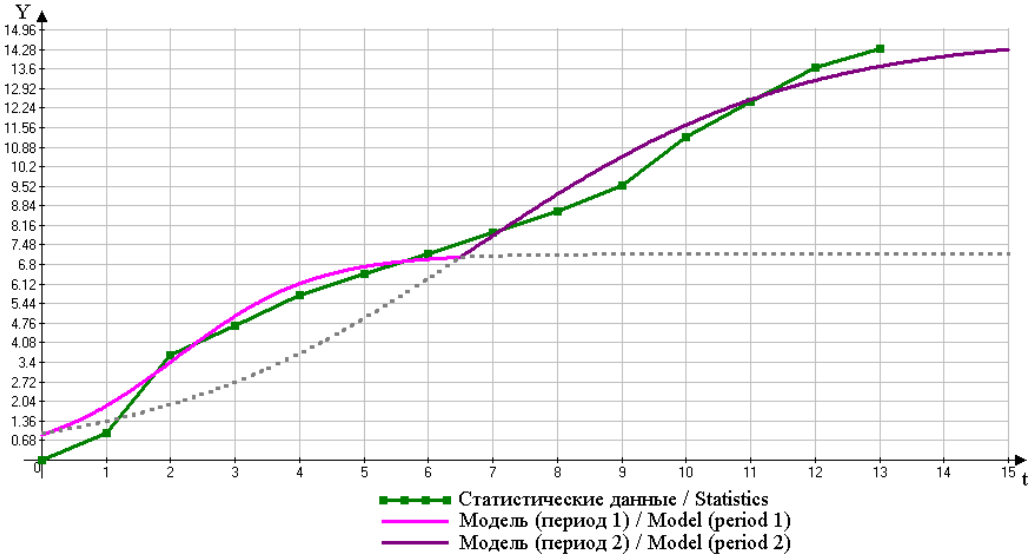
**The average dissemination time of the II idea in clusters**

| № кластера / Number of cluster | Среднее время распространения идеи ИВ, ч / Average time of disseminating the II idea, in hours |
|---|---|
| 1-й кластер / Cluster 1 | 310,00 |
| 2-й кластер / Cluster 2 | 250,40 |
| 3-й кластер / Cluster 3 | 181,00 |
| 4-й кластер / Cluster 4 | 133,25 |
| Индивидуальный объект / The individual object | 62,00 |

что независимые параллельные процессы информационного воздействия в однородных независимых популяциях протекают со схожей динамикой и параметрами модели, описывающей эти процессы.

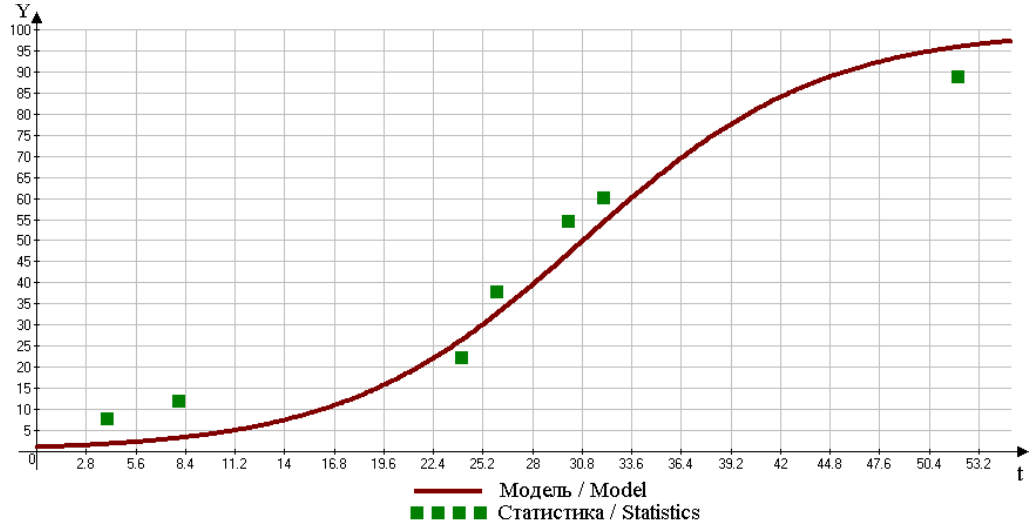
Эксперимент по распространению идеи ИВ проводился в студенческой среде (рис. 11). В качестве объектов для распространения идеи ИВ выбраны семь независимых студенческих групп, обучающихся в различных вузах медицинского профиля. Вероятность контакта между участниками групп принималась равной нулю в силу специфики организации образовательного процесса.

Таким образом, экспериментальные исследования системно-динамических моделей с использованием реальных статистических данных о распространении ИВ подтвердили их эффективность и работоспособность для прогнозирования динамики распространения ИВ в зависимости от скорости инфор-




Р и с. 10. Моделирование динамики распространения в социальной сети ИВ о проведении оппозиционных митингов

F i g. 10. Modeling the dynamics of disseminating the information about opposition rallies in the social networks




Р и с. 11. Результаты эксперимента по распространению ИВ в студенческой среде

F i g. 11. The experimental results of disseminating II to students

мационного «заражения», особенностей социальных групп, топологии социальных сетей и других факторов.

**Обсуждение и заключение**

1. Для решения задач исследования негативных ИВ на социальные группы и процессов информационного противоборства, а также управления этими процессами эффективно применение методов системно-динамического, агентного и дискретно-событийного моделирования, используемого на сегодняшний день для исследования различных сложных социально-экономических процессов.

2. Имитационные модели ИВ и ИПД позволяют оценивать, анализи-

ровать и прогнозировать использование социальных сетей в качестве среды распространения экстремизма, терроризма, молодежной агрессии, аутоагрессии и других крайне опасных явлений. Результаты расчетов с помощью системы уравнений, реализованной в имитационной системе Anylogic, дают возможность территориальным органам управления и силовым структурам заблаговременно обосновывать управленческие решения по подготовке и реализации мероприятий, направленных на снижение или нейтрализацию указанных негативных ИВ на общество в целом и его социальные группы (включая молодежь) в частности в зависимости от структуры и динамики факторного комплекса, влияющего на процессы ИВ в социальных сетях.

3. Выбранное в качестве среды моделирования программное обеспечение современных имитационных платформ позволяет в деталях проигрывать различные сценарии с использованием системно-динамических и агентных моделей, наглядно интерпретировать результаты моделирования, проводить различные виды имитационных экспериментов.

4. Топологические различия социальных сетей как современной платформы ИВ и ИПД могут эффективно использоваться для построения стратегии и тактики информационного контакта с населением со стороны региональных властей и силовых структур, а также для более четкого и обоснованного построения системы противодействия различным негативным информационным влияниям на социальные группы, особенно молодежные, со стороны окружения различной природы, осуществляющего информационные операции.

5. Новизна модели информационного противоборства связана с тем, что в имитационной системе впервые описываются две противоборствующие идеи (имитационная платформа позволяет учитывать их любое разумное количество). Новым, пока не использованным в моделях информационных операций, является подход с применением к социальным процессам постулата Гиббса из статистической физики.

6. Перспективой развития анализа топологических различий в рамках системно-динамического подхода является выявление дополнительных «глубинных» факторов, характеризующих разные поселения/города/регионы и влияющих на динамику распространения идеи ИВ.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Как управлять массовым сознанием: современные модели / В. А. Минаев [и др.]. М. : РосНОУ, 2013. 200 с.

2. **Минаев В. А., Дворянкин С. В.** Моделирование динамики информационно-психологических воздействий на массовое сознание // Вопросы кибербезопасности. 2016. № 5 (18). С. 56–64. DOI: https://doi.org/10.21681/2311-3456-2016-5-56-64

3. **Минаев В. А., Дворянкин С. В.** Обоснование и описание модели динамики информационно-психологических воздействий деструктивного характера в социальных сетях // Безопасность информационных технологий. 2016. Том 23, № 3. С. 40–52. URL: https://bit.mephi.ru/index.php/bit/article/view/16/26

4. Моделирование угроз информационной безопасности с использованием принципов системной динамики / В. А. Минаев [и др.] // Вопросы радиоэлектроники. 2017. № 6. С. 75–82.

5. **Губанов Д. А., Новиков Д. А., Чхартишвили А. Г.** Социальные сети: модели информационного влияния, управления и противоборства / под ред. чл.-корр. РАН Д. А. Новикова. М. : ФИЗМАТЛИТ, 2010. 228 с.

6. Системно-динамическое моделирование информационных воздействий на социум / В. А. Минаев [и др.] // Вопросы радиоэлектроники. 2017. № 11. С. 35–43.

7. **Алехнович С. О., Слизовский Д. Е., Ожиганов Э. Н.** Системно-динамическое моделирование: принципы, структура и переменные (на примере Московской области) // Вестник РУДН. Серия «Политология». 2009. № 1. С. 22–36. URL: http://journals.rudn.ru/political-science/article/view/8918/8369

8. **Liu W., Cui Y., Li. Y.** Information systems security assessment based on system dynamics // International Journal of Security and Its Applications. 2015. Vol. 9, no. 2. P. 73–84.

9. **Kim A. C., Lee S. M., Lee D. H.** Compliance risk assessment measures of financial information security using system dynamics // International Journal of Security and Its Applications. 2012. Vol. 6, no. 4. P. 191–200.

10. **Behara R., Derrick Huang C., Hu Q.** A system dynamics model of information security investments // Journal of Information System Security. 2010. Vol. 6, no. 2. P. 1572–1583. URL: https://pdfs.semanticscholar.org/5e4d/6276a8788cc43c1bb0531be97eec24490f94.pdf

11. **Гусаров А. Н., Жуков Д. О., Косарева А. В.** Описание динамики распространения компьютерных угроз в информационно-вычислительных сетях с запаздыванием действия антивирусов // Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». 2010. № 1 (78). С. 112–120. URL: http://vestnikprib.ru/articles/122/122.pdf

*Поступила 05.12.2018; принята к публикации 21.01.2019; опубликована онлайн 29.03.2019*

*Об авторах:*

**Минаев Владимир Александрович**, профессор, кафедра защиты информации, ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана» (105005, Москва, ул. 2-я Бауманская, д. 5, стр. 1), доктор технических наук, ResearcherID: B-4420-2016, ORCID: https://orcid.org/0000-0002-5342-0864, m1va@yandex.ru

**Сычев Михаил Павлович**, профессор, кафедра защиты информации, ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана» (105005, Москва, ул. 2-я Бауманская, д. 5, стр. 1), доктор технических наук, ResearcherID: E-1068-2019, ORCID: https://orcid.org/0000-0002-7535-7704, mpsichov@sm.bmstu.ru

**Вайц Екатерина Викторовна**, доцент, кафедра защиты информации, ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана» (105005, Москва, ул. 2-я Бауманская, д. 5, стр. 1), кандидат технических наук, ResearcherID: D-9164-2019, ORCID: https://orcid.org/0000-0002-4629-6252, vaitcev@yandex.ru

**Бондарь Константин Михайлович,** профессор, кафедра информационного и технического обеспечения органов внутренних дел, Дальневосточный юридический институт МВД России (680020, г. Хабаровск, пер. Казарменный, д. 15), кандидат технических наук, доцент, ResearcherID: D-9910-2019, ORCID: https://orcid.org/0000-0002-6928-0413, bondar_km@mail.ru

*Заявленный вклад соавторов:*

В. А. Минаев – математическое описание моделей, формулирование задач, обсуждение результатов; М. П. Сычев – обоснование имитационной платформы, формулирование выводов; Е. В. Вайц – проведение имитационных экспериментов, описание результатов; К. М. Бондарь – обзор литературы, анализ результатов исследования.

*Все авторы прочитали и одобрили окончательный вариант рукописи.*

## REFERENCES

1. Minaev V.A., Ovchinskiy A.S., Skryl S.V., Trostyanskiy S.N. [How to manage mass consciousness. Modern models]. Moscow: Russian New University; 2013. (In Russ.)

2. Minaev V.A., Dvoryankin S.V. Modeling the dynamics of information and psychological influence on mass consciousness. *Voprosy kiberbezopasnosti* = Cybersecurity Issues. 2016; 5:56-64. DOI: https://doi.org/10.21681/2311-3456-2016-5-56-64 (In Russ.)

3. Minaev V.A., Dvoryankin S.V. Foundation and description of informational and psychological destructive nature influences dynamics model in social networks. *Bezopasnost informatsionnykh tekhnologiy* = IT Security. 2016; 23(3):40-52. Available at: https://bit.mephi.ru/index.php/bit/article/view/16/26 (In Russ.)

4. Minaev V.A., Sychev M.P., Vaits E.V., Gracheva Y.V. Modeling of threats to information security using principles of system dynamics. *Voprosy radioelektroniki* = Questions of Radio Electronics. 2017; 6:75-82. (In Russ.)

5. Gubanov D.A., Novikov D.A., Chkhartishvili A.G. [Social networks: models of information influence, management and confrontations]. Moscow: Publishing House of Physical, Mathematical and Technical Literature; 2010. (In Russ.)

6. Minaev V.A., Sychev M.P., Vaits E.V., Kirakosyan A.E. System-dynamic modeling of information influences on society. *Voprosy radioelektroniki* = Questions of Radio Electronics. 2017; 11:35-43. (In Russ.)

7. Alekhnovich S.O., Slizovskiy D.E., Ozhiganov E.N. System-dynamical modeling: the principles, structure and variables (on the example of the Moscow region). *Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Politologiya* = Bulletin of Peoples' Friendship University of Russia. Series: Political Science. 2009; 1:22-36. Available at: http://journals.rudn.ru/political-science/article/view/8918/8369 (In Russ.)

8. Liu W., Cui Y., Li. Y. Information systems security assessment based on system dynamics. *International Journal of Security and Its Applications.* 2015; 9(2):73-84.

9. Kim A.C., Lee S.M., Lee D.H. Compliance risk assessment measures of financial information security using system dynamics. *International Journal of Security and Its Applications*. 2012; 6(4):191-200.

10. Behara R.S., Derrick Huang C. A System dynamics model of information security investments. *Journal of Information System Security*. 2010; 6(2):1572-1583. Available at: https://pdfs.semanticscholar.org/5e4d/6276a8788cc43c1bb0531be97eec24490f94.pdf

11. Gusarov A.N., Zhukov D.O., Kosareva A.V. Description of dynamics of computer threats propagation in data computer networks with delay of antivirus software operation. *Vestnik MGTU im. N. E. Baumana. Ser.: Priborostroyeniye* = Herald of the Bauman Moscow State Technical University. Series Instrument Engineering. 2010; 1:112-120. Available at: http://vestnikprib.ru/articles/122/122.pdf (In Russ.)

*Submitted 05.12.2018; revised 21.01.2019; published online 29.03.2019*

*About the authors:*

**Vladimir A. Minaev**, Professor, Department of Information Security, Chair of Information Protection, Bauman Moscow State Technical University (2nd 5, bd. 1 Baumanskaya St., Moscow 105005, Russia), D.Sc. (Engineering), ResearcherID: B-4420-2016, ORCID: https://orcid.org/0000-0002-5342-0864, m1va@yandex.ru

**Mikhail P. Sychev**, Professor, Department of Information Security, Chair of Information Protection, Bauman Moscow State Technical University (2nd 5, bd. 1 Baumanskaya St., Moscow 105005, Russia), D.Sc. (Engineering), ResearcherID: E-1068-2019, ORCID: https://orcid.org/0000-0002-7535-7704, mpsichov@sm.bmstu.ru

**Ekaterina V. Vaits**, Associate Professor, Department of Information Security, Chair of Information Protection, Bauman Moscow State Technical University (2nd 5, bd. 1 Baumanskaya St., Moscow 105005, Russia), Ph. D. (Engineering), ResearcherID: D-9164-2019, ORCID: https://orcid.org/0000-0002-4629-6252, vaitcev@yandex.ru.

**Konstantin M. Bondar**, Professor, Department of Information and Technical Support of Internal Affairs, Far Eastern Law Institute of the Ministry of Internal Affairs of the Russia (15 Kazarmennyy Pereulok, Khabarovsk 680020, Russia), Ph.D., Associate Professor, ResearcherID: D-9910-2019, ORCID: https://orcid.org/0000-0002-6928-0413, bondar_km@mail.ru.

*Contribution of the authors:*

V. A. Minaev – mathematical description of the models, formulation of the problems, discussion of the results; M. P. Sychev – justification of the simulation platform, formulation of conclusions; E. V. Vaits – simulation experiments, description of the results; K. M. Bondar – literature review, analysis of the research results.

*All authors have read and approved the final version of the paper.*